protection but not select a particular compliant solution.[48] Manufacturers should have the option of satisfying such standards through self-certification and, to ensure insure innovative technologies and competition have a chance to develop, the standard should not become effective until a minimum number of solutions have been certified and manufacturers have had sufficient time to incorporate them in their products. In addition, the Commission will need to adopt so called "robustness" rules to guide the effectiveness of the protection scheme. Such robustness standards should be aimed at the ordinary consumer, not an expert, determined hacker and expressed in terms of frustrating circumvention of the system. The FCC's action will also need to ensure that, under any new protection scheme, programming that enhances civic discourse remains available. Finally, as also discussed below, any scope of protection that the FCC defines to govern redistribution should prevent the unauthorized redistribution of marked digital terrestrial broadcast television to the public.

A. If the Commission Determines, Despite the Numerous Legal and Administrative Infirmities, That Regulating Authorized Output and Recording Technologies Is Required, It Should Do No More Than Establish Objective, Technical, and Licensing Criteria for Such Authorized Technologies

If the Commission decides to adopt a content protection scheme, the Commission can be guided by the "high level" consensus the BPDG participants reached regarding the issue of recording and output of content from products subject to a broadcast flag system. Such consensus was the by-product of years of discussion among the affected industries.

[48] Throughout this document, use of the phrase "objective, technical and licensing criteria" is not intended to preclude the establishment of other means of selection, such as marketplace acceptance, as agreed by affected parties.

As set forth in the *BPDG Final Report*, the BPDG participants agreed that unscreened and marked content should be recorded or output from “covered products” only by four permitted methods.” Three of the permitted methods were clearly stated by their terms and required no further discussion or agreement. The first permitted category involved analog output and analog recording methods,’” a category which all participants could agree should not be subject to restrictions because of the existence of numerous legacy analog devices. The second category involved n-VSB and m-QAM modulators,[51] a category which all participants could also agree should not be subject to additional controls because the demodulation of such content was already addressed and protected under other aspects of a broadcast flag system.” The third category involved unprotected DVI outputs (at limited resolutions), or digital outputs from computers,[53] which the participants again agreed should not be controlled because of the existence of numerous legacy devices.

The focus of most of the BPDG’s work was the fourth category, treatment of digital output and recording methods. The BPDG participants reached consensus on a generalized statement but could not fully agree on specification of particulars. As a general matter, it was agreed that any copy protection regime should allow recording or

[49] *BPDG Final Report* at § 4.6.

[50] *Id.* at § 4.6 a.

[51] *Id.* at § 4.6 h. Agreement to this category would he “subject to requirement of conditions,” which participants believed could be easily resolved.

”*Id.* at § 4.3.

[53] *Id.* at § 4.6 c.

outputting of unscreened and marked content via "[d]igital outputs and recording methods that provide specified levels of protection against unauthorized redistribution."[54] But there was not full agreement on the particulars of how to accomplish this goal. The authorized digital output and recording methods embodied within this broad category were to be set forth in a "Table A" to the "requirements document" that accompanied the *BPDG Final* ***Report.*** The participants, however, could not agree on key elements of the technologies and how they would qualify for inclusion in Table A.

First, if the FCC decides to mandate a content protection regime, as part of establishing the objective, technical, and licensing criteria that will govern compliant solutions, the agency will need to focus on three key elements that such content protection solutions must address: rights expression, encryptioddecryption, and authentication. Rights expression is the ability to convey the level of protection to be afforded the content. The broadcast flag itself is a simple example of rights expression. Encryption/decryption is a well established technology, widely used for many purposes when security and protection of information are required, which could be used to give effect to rights expression to ensure protection. Authentication provides the verification necessary for any content protection system to function successfully. Sample suggested objective, technical, and licensing criteria for each of these specific elements are set forth in Appendix B to these comments.

Second, any process that the FCC adopts to select such solutions should be straightforward and transparent and should include certain basic features that can be

[54] *Id.* at § 4.6 d.

applied in a manner that does not restrain markets. The BPDG participants had extensive discussions evaluating selection criteria but did not resolve the issue." One standard that BPDG participants debated included criteria, which would have made the initial selection of authorized solutions subject to explicit ‘‘use’’ or "approval" of a technology by a varying number of movie studio representatives.[56] The information technology industry preferred the addition of a more neutral process pursuant to which one constituency would not have the ability to decree a particular solution; therefore, technology participants advocated the addition of general functional standards that would be specified by the entity tapped to enforce the broadcast flag system, and manufacturers would have the flexibility to design products that met those standards."

The selection process preferred by the computer industry involves self-certification with review procedures that an affected party may invoke if it believes that the certification is inappropriate. Under this approach, once a solution is ready for market, the vendor would file a notice with the Commission that its output or recording solution meets the **rule's** objective criteria. Affected parties would be able to object to

[55] *BPDG Final Report* at **$6.8.**

[56] *BPDG Final Report,* Tab F-1. Of the four proposed procedures, two directly required such studio assent. One required assent by *"3* Major Studios and/or Major Television Broadcast Groups (of which at least *2* must be Major Studios)." *Id.* at 2, "Proposed Criteria," § (1). The other required assent by at least "2 Major Studios." *Id.* at § *(2)*. **A** third procedure involved elements that assumed that a technology would already be listed on Table **A,** thereby interjecting the need for movie studio assent pursuant to either of the two previously described procedures. *Id.* at § *(3)*.

[57] *Id.* at § (4). The fact that the information technology industry was willing to agree to the same document that embodied the content industry's three other preferred selection methodologies turned on the fact that the various selection methods set forth in the document were phrased in the disjunctive.

the self-certification, and if no objections were tiled within a reasonable time, manufacturers would be able to begin to use that technology to comply with the rules.

As part of such system, the Commission should establish a clear and predictable process for reviewing any objections that may be filed on a fast track schedule. If a challenger alleges a technical failure to meet the objective criteria, the solution should be examined by the FCC’s Office of Engineering and Technology. If the alleged failure relates to licensing terms and conditions, then the FCC’s Office of the General Counsel should review the license terms and conditions. Resolution of the objection should be expeditious to avoid disruptions in the marketplace, and generally should not take more than sixty (60) days.

This system of objective, technical, and licensing criteria and straightforward, transparent selection will result in the maximum number of compliant solutions, which in turn will foster competition among technology companies, spur innovation, lower prices, and increase consumer convenience. Competition among compliant solutions will also improve ease of use and interoperability since market forces will pressure device manufacturers to select protection schemes that communicate with each other.” Overall, objective criteria and a transparent selection process will benefit content providers by ensuring effective operation of the broadcast flag system.

[58] Market forces have traditionally driven consumer product manufacturers toward interoperability. The eventual triumph of VHS technology over Sony’s Betamax technology is an example of the market rewarding format interoperability and punishing a proprietary format. On the other hand, Macintosh has remained in the market by data exchange interoperability, *i.e.*, file exchange and networking compatibility with Windows products.

B. The New Rules Should Not Become Effective Until There Is Choice in the Marketplace, a Minimum Number of Solutions Is Certified, and Manufacturers Have Sufficient Time To Incorporate Them in Products

The IT Coalition also has concerns about the timing of the effective date of any new broadcast flag rules that may be adopted. If the FCC permits the broadcast flag rules to become effective after only one or two authorized output and one or two authorized recording technologies are certified, it may risk curtailing choice and competition. In addition, once a sufficient number of compliant solutions has been established, manufacturers should be given a reasonable time to incorporate those solutions into their products and manufacture and distribute them.

Intense and vigorous competition among analog TV set manufacturers has resulted in extremely low prices for analog receivers over the last decade. As a result, a 27-inch television today retails for under $230.[59] It is imperative that competition among DTV set manufacturers also be allowed to flourish and that the FCC not take any actions that would stymie that competition.

Upon adoption of a rule governing DTV sets, manufacturers, realizing they must comply, will likely choose among whatever compliant solutions are then available and will incorporate their selection in devices as soon as possible so that they have uninterrupted production of DTV sets and remain competitive with other manufacturers. To ensure such competition continues, manufacturers should not be required to license a

[59] See, *e.g.*, RCA 27" Stereo TV with GUIDE PLUS+ Gold - F27442, $229.50, http://www.bestbuv.com/HomeAudioVideo/Televisions/MidsizeTV129.asp?m=1&cat=24&scat=27 (last visited Nov. 26, 2002).

compliant solution until there are a minimum number of such solutions available for selection.

Once a sufficient number of solutions is qualified, manufacturers need adequate time to incorporate those compliant solutions into their products. The first step is reviewing and agreeing to a license between the private parties. The second step is redesigning existing products to incorporate the technology. The third step is changing manufacturing processes to accommodate the new design. The final step is producing the products and moving them into the manufacturing and inventory pipeline.[60] Any rules adopted by the FCC should not become effective until a sufficient amount of time has elapsed to allow a diverse array of compliant solutions to develop

C. The BPDG's Robustness Rules Must Be Reformed To Ensure That They Do Not Unreasonably Burden Devices and Manufacturers

Robustness is the methodology for preventing unauthorized access to content. Two general categories of robustness exist. The first is content protection robustness, which gauges the strength and effectiveness of the encryption or scrambling that has been applied to transmitted content to prevent access to that content by unauthorized persons.'' The second type of robustness is device robustness, which involves the ability of a receiver or downstream product which has received protected content to prevent unauthorized access to that content when it is in an unprotected state inside the receiver

[60] The rule should also permit the sale of inventoried non-compliant products for **a** reasonable period such as one year.

[61] Objective criteria for compliant solutions will set this robustness level.

or the downstream device.[62] This robustness measure specifies how resistant the receiver or such downstream product is to efforts to gain access to that content in its unprotected state. The level of resistance directly affects product cost and performance.[63]

While the BPDG participants did address device robustness, they failed to reach consensus on all aspects of the issue. Accordingly, if the FCC decides that it no longer wants to rely on industry forces and needs to regulate in this area, it will need to set device robustness requirements. The IT Coalition believes that, if the FCC does so, it should select a reasonable level of resistance, one that is not so high as to markedly increase cost and lower performance, but one that is still sufficient to provide **an** acceptable level of protection.[64]

[62] In most systems, the content at one point or another will exist in an unprotected format inside the device. In a DVD CSS player, for example, the compressed scrambled MPEG-2 video must be unscrambled so that the MPEG decoder may convert the compressed MPEG code into video output for display on a TV screen. Accordingly, the DVD CSS Procedural Specifications require that devices be manufactured and software written in such a way that a user cannot readily access the unscrambled MPEG video. *See, e.g.*, DVD Content Protection Ass'n, *Content Scramble System Specifications, Procedural Specifications* §§ 6.2.4. – 6.2.6. (copy available at http://www.dvdcca.org/css/application_proc.html)

[63] Hardware, for example, can be secured with a special case that can only be opened with tools not generally available to the public. Software can be secured by a variety of techniques resulting in "tamper resistant code." One way to provide tamper resistance is "obfuscation," a method of scrambling code so that standard software debugging tools are unable to read it. All such techniques increase product and support costs. For example, hardware protection usually results in increased manufacturing costs. Software coding techniques require increased programmer time both to write the original code and to find and correct software errors. In addition, tamper resistant code requires more processing power to run (*i.e.*, more expensive chips).

[64] Because DTV broadcast material will be delivered over-the-air in the clear, it would not be reasonable to require as high a robustness level as provided for DVDs, for example, which are delivered in a scrambled protected form. Moreover, the content on newly released DVDs is generally not available free over-the-air.

In addressing the issue, the FCC will need to consider that device robustness levels can he measured by three standards. The first specifies the tools against which the device must be resistant. The second references the attacker's skill. The final standard establishes the level of effort needed to overcome the system, an acknowledgement of the fact that any protection system will ultimately be defeated. The BPDG participants reached consensus as to the type of tools a device should be able to resist.[65] Full consensus was not reached, however, as to the skill of the attacker and the level of effort that should be specified for circumventing the system.[66]

During the BPDG sessions, content industry participants argued that the robustness level should be set to frustrate an attack by anyone regardless of his or her skill level. To meet this standard, a device would essentially have to be designed and produced so as to frustrate attack by even the most highly skilled professional.[67] Some argued that such a standard would increase the cost of DTV equipment, and some in the IT Coalition would prefer that the FCC instead set the standard by reference to the skill of an ordinary consumer or user, not an expert. To do otherwise would require a manufacturer designing a DTV receiver to consider that the potential hacker could he an experienced electronic engineer using tools like EEPROM readers and writers, debuggers, decompilers, or similar devices. Some argue that assuming anything but an

[65] *Requirements Document ut* §X.11

[66] *Id.* at X.7(a), X.9(b)(2) & (c)(2), and X.11(a).

[67] All parties anticipate professional DTV receivers will be exempt from the Broadcast Flag requirements. *(See BPDG Final Report* at §4.12). Accordingly, it is unreasonable to require that devices for sale to the general public be resistant to attack by professionals who may acquire receivers not subject to the robustness rules.

ordinary level of skill is unreasonable for a mass-marketed consumer device and would result in higher receiver prices and increased burdens on the average consumer. **A** standard of this level would be consistent with the goal of the broadcast flag which is to "keep the honest users honest" by preventing unrestricted public access to free programming originally transmitted in the clear.

During the BPDG discussions, content providers also argued that the level of difficulty should be set at "effectively frustrating" attempts to hack a product. The goal should he to ensure that technologies frustrate persons with ordinary skills rather than experts.[68] Accordingly, the IT Coalition urges the Commission to adopt a requirement that incorporates this concept. This would allow manufacturers to take reasonable steps to prevent average consumers from defeating the protections

D. The FCC Should Not Regulate Consumer Digital Modulators at This Time

If the FCC promulgates DTV content protection rules, it will also need to determine whether it should extend the broadcast flag rules to consumer digital modulators, a concept which the BPDG participants did not originally consider as part of the broadcast flag rules.[69] Suggested during the discussions by some studios, this proposal was not intended to protect DTV broadcast material. Rather, it reflected a concern that if an effective additional DVD protection mechanism were to he adopted by

[68] Hackers enjoy hacking like golfers enjoy golfing. While it might not make sense to the uninitiated, the fun is in the challenge. The brass ring of cracking the FCC's "approved" digital content protection system would he the hacker equivalent of playing Pebble Beach. With so many hackers willing to take a swing at breaking the protection scheme, eventually one is bound to succeed and find a hole.

the DVD CCA, for example, the broadcast flag system would become an unintended conduit for illegally distributed DVD content.[70]

This proposal suffers from several notable infirmities. First, because the proposal was not considered in detail before the final BPDG meeting, industry participants were unable to evaluate the cost and performance burdens associated with it. Second, the proposal raised concerns just before the BPDG discussions were completed that an apparent "hole" in the system was discovered necessitating the proposed extension of the rule to a broad array of consumer products. Such extension is exactly the kind of regulatory accretion or "creep" that concerns the computer industry. Third, to date, no content marking system has been adopted by an industry-based voluntary standards setting body, nor does adoption of one appear to be on the horizon in the near term." If the Commission adopts a broadcast flag rule and if at some future time DVD CCA adopts a content marking system, the FCC could then consider whether it is appropriate to add the regulation of consumer modulators to the regulation of DTV receivers.

[69] *BPDG Final Report* at §5.9.

[70] The theory is that if (a) an effective secondary DVD content protection system using content marking, such as watermarks, were adopted, and (b) an individual bypassed DVD CSS, he or she could "launder" the content by masquerading it as broadcast material when rebroadcast through a consumer modulator. This would permit the individual to play material that he or she would not be able to play through a "compliant" DVD Player.

[71] See the August 12,2002 announcement by DVD CCA at http://www.dvdcca.org/ (last visited Dec. 6, 2002), reporting that its efforts to select a content marking system had been unsuccessful. Given the inherent limitations of such marking systems, it is not likely that a "consensus" system will be selected anytime soon. If a secondary DVD content protection system is adopted, any existing FCC rules could be amended to accommodate such a system, if necessary.

E. The Commission Should Consider and Adopt Encoding Rules That Ensure Programs Which Enhance Civic Discourse and Promote the Public Interest Will Be Fully Available

So called "encoding" rules determine when content owners may or may not apply **a** content protection system. Generally, the IT Coalition believes that content providers should be permitted, at their discretion, to decide whether to apply the broadcast flag to a given program or to refrain from inserting the flag. The IT Coalition cannot envision any instances in which the Commission should order that programs be protected against redistribution.

On the other hand, civic discourse would be enhanced and the public interest would be served if access to certain programming, such as news and public affairs, is not impeded, and such programming remains widely available. For example, a broadcaster should not be allowed to prevent redistribution of the President's State of the Union Address or candidate debates. The Commission should consider adopting provisions that ensure such access as being in the public interest.''

F. The Scope of Protection Should Be To Prevent Unauthorized Access to Marked Digital Terrestrial Broadcast Television by the Public

The BPDG participants were unable to agree upon the boundaries or scope of protection for the broadcast flag system.[73] During the course of their evaluation, scope **was** described in various ways, including "protection against unauthorized redistribution (including the Internet)" or "unauthorized redistribution outside the home or personal

[72] Standards that assure access based on content will likely require legislation. See discussion of *MPAA v. FCC*, *supra,* Section **ILA.**

[73] *BPDG Final Report* at § 5.1.

digital network environment,” or outside the “home or other similar local environment.””
BPDG participants engaged in considerable discussion as to whether and how consumers, as they currently may do with today’s analog television programming, could transfer DTV material to their offices, vehicles, second homes, or other personal environments. Despite lengthy discussions, the BPDG participants were unable to agree on how to define the scope of protection.

Americans watch a considerable amount of television, and analog technology has enabled reasonable viewer flexibility. **As** a technical matter, digital technology is able to offer even greater flexibility, which will help spur adoption of DTV. If consumers’ current untrammeled flexibility were to be curtailed by a restrictive definition of scope of protection, the DTV transition would suffer appreciably.

The scope of protection will directly affect consumers’ DTV experience. Thus, the FCC should carefully define the scope of protection to be afforded heretofore-unprotected terrestrial DTV broadcast signals. The goal should be to promote consumer adoption of DTV, not create disincentives to adoption. Scope is best defined in terms of who may access copy in usable form, rather than when, how, where and which copies may be made. This is the concept of scope that is successfully employed in the DVD CSS context. Under this approach, while it is actually possible to make unlimited copies of scrambled DVD discs, such copies are unusable without an authorized key.

Defining the scope as preventing the unauthorized access to marked digital terrestrial broadcast television by the public would have a number ofbenefits. First, it

[74] ***Id.***

would promote the ability of consumers to continue enjoying DTV as they enjoy analog TV today. Second, it would ensure that product manufacturers are not unreasonably burdened by costs passed on to consumers. Third, it will ensure that DTV home networking will be innovative and stimulate the demand for DTV accelerating the transition from analog to digital broadcasting. We support this definition and believe it strikes a reasonable balance between protecting DTV content from unauthorized access and unduly impeding consumer adoption of DTV.

IV. Conclusion

The IT Coalition has substantial reservations about the FCC's proposal to adopt a broadcast flag content protection scheme for DTV signals, principally because it believes that the FCC does not currently have delegated authority to take such action. If the FCC chooses to regulate in this area, it will be acting on very tenuous ground. If the FCC concludes, however, that such regulation is within its jurisdiction, the agency should proceed as narrowly as possible following the recommendations set forth above.

Respectfully submitted,

BUSINESS SOFTWARE ALLIANCE
COMPUTER SYSTEMS POLICY
PROJECT

By
James M. Burger
M. Anne Swanson

of

Dow, Lohnes & Albertson, PLLC
1200 New Hampshire Avenue, N.W
Suite 800
Washington, DC 20036
(202) 776-2534

Their Attorney

December 6,2002

APPENDIX A

BSA
BUSINESS SOFTWARE ALLIANCE

BSA Digital Television Compendium
December 2,2002

As part of an effort to quantify the availability of digital television programming and information in the United States, the Business Software Alliance created this compendium. Primary data sources included the websites of the National Association of Broadcasters, the Consumer Electronics Associations, the four major networks, and online digital programming guides such as HDTV Magazine and TitanTV.

Digital television signal accessibility

According to the National Association of Broadcasters list of stations broadcasting in DTV, as of December 2,2002,621 stations in 167 markets are now broadcasting in DTV.' This covers approximately 94% of the American population. According to the National Association of Broadcasters, 62% of Americans also reside in markets where 5 or more stations broadcast digitally? This is a significant increase from the beginning of 2002 when only 229 stations in 80 markets were broadcasting digitally covering only 73% of Americans.[3]

Digital television broadcast marketing

Two networks, ABC and CBS, announced the sponsorships of their HDTV programming in August 2002 by the consumer electronics company Zenith[4] [5]. The National Association of Broadcasters and the Consumer Electronics Association have jointly sponsored the DigitalTVZone at http://www.digitaltvzone.com to provide consumers with information about Digital television including local events. The Consumer Electronics Association has also sponsored AntennaWeb at http://www.antennaweb.org to identify the appropriate over the air antenna for consumers at their receiving location.

Digital television signal broadcasting

All four of the major television networks broadcast some or all of their new prime time programming digitally, if not in enhanced or high definition format. This programming has increased significantly in the 2002-2003 season. Most repeats and some movies are not broadcast in enhanced or high definition format.

[1] http://www.nab.org/Newsroom/issues/digitaltv/DTVStations.asp - **link reviewed December** 2,2002

[2] http://www.nab.org/Newsroom/Pressrel/releases/6902.htm - **link reviewed December** 2, 2002

[3] http://www.nab.org/Newsroom/pressrel/releases/0202.htm - **link reviewed December** 2,2002

[4] http://www.abcmedianet.com/pressrel/dispDNR.html?id=082802_01 and http://www.zenith.com/sub_news/news_Display.asp?action=view&id=465&cat=&year – **links reviewed December** 2,2002

[5] http://www.zenith.com/sub_news/news_Display.asp?action=view&id=466&cat=&year - **link reviewed December** 2.2002

	Total primetime hours in EDTV/HDTV	Percentage of primetime broadcasts in digital[6]	Percentage of prime time broadcasts in EDTV/HDTV
ABC[7]	13.5 of 21	64%	64%
CBS[8]	17 of 21	100%	
Fox[9]	14 of 14	100%	100%
NBC[10]	9.5 of 21		

Detailed network by network programming information follows. Note that several network owned and produced shows that could be broadcast digitally are not. Broadcasting these shows produced by the networks themselves would further increase the amount of digital content available to Americans.

[6] Beginning September 23, 2002, CBS broadcasts all of its primetime programming in digital even if the content is not EDTV or HDTV.

[7] Not all ABC movies are broadcast digitally.

[8] CBS also broadcasts the **Young** and the Restless, daytime's #1 ranked drama in HDTV. While all CBS primetime movies are broadcast in digital form, not all are broadcast in HDTV.

[9] **Fox** also broadcasts **at** least one NFL game in EDTV every week.

[10] NBC also broadcasts The Tonight Show with **Jay** Leno and The Conin O'Brian Show in HDTV.

ABC 2002-2003 Primetime Season (HDTV in green)

	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
8:00	Drew Carey	8 Simple Rules	My Wife And Kids	Dinotopia	Funniest Home Videos	ABC Big Picture Show	Wonderful World Of Disney
8:30	Whose Line Is It Anyway	According To Jim	George Lopez				
9:00	Monday Night Football	Life With Bonnie	The Bachelor	Push Nevada	That Was Then		Alias
9:30		Less Than Perfect					
10:00		NYPD Blue	MDs	Primetime Thursday	20/20		The Practice
10:30							

NETWORK PRODUCED SHOW NOT IN HDTV

ABC broadcasts at least 13.5 hours per week in HDTV.

HDTV movies have included Armageddon, Backdraft, A Bug's Life, Beauty and The Beast, Doctor Doolittle, Enemy of the State, The Green Mile, Liar Liar, Notting Hill, Pinocchio, Prince William, The Santa Clause, Saving Private Ryan, The Sixth Sense, and Toy Story 2.

Upcoming sports programs will include the 2003 Super Bowl, NBA finals, and the NHL's Stanley Cup. The 2003-2004 season of Monday Night Football will also be broadcast in HDTV, ESPN's HDTV channel will debut in April 2003.

Previous HDTV sports programs have included the 2000 SuperBowl and NHL All-Star Game and the 1999-2000 season of Monday Night Football.

CBS 2002-2003 Primetime Season (HDTV in green)

	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
8:00	King of Queens	JAG	60 Minutes	Survivor	48 Hours	Touched by an Angel	Becker
8:30	Yes, Dear						King of Queens
9:00	Everybody Loves Raymond	The Guardian	The Amazing Race	CSI	Hack	The District	CBS Sunday Movie (partial)
9:30	Still Standing						
10:00	CSI: Miami	Judging Amy	Presidio Med	Without A Trace	The Agency	Robbery Homicide Division	
10:30							

NETWORK PRODUCED SHOW NOT IN HDTV

CBS broadcasts at least 18 hours per week in HDTV, 17 of which are in primetime.

On August 28,2002, CBS Television announced that it will offer all 18 of its primetime comedies and dramas in HDTV in the upcoming 2002-2003 television season along with selected movies. Beginning September 23, 2002, all CBS primetime programming will be broadcast from the tower in DTV, either in HDTV or in SDTV.

Other CBS HDTV broadcasts include daytime's #1 ranked drama, The Young and the Restless, the U.S. Open, the NCAA Final Four, and the Master's golf tournament.

NBC 2002-2003 Primetime Season (HDTV in green)

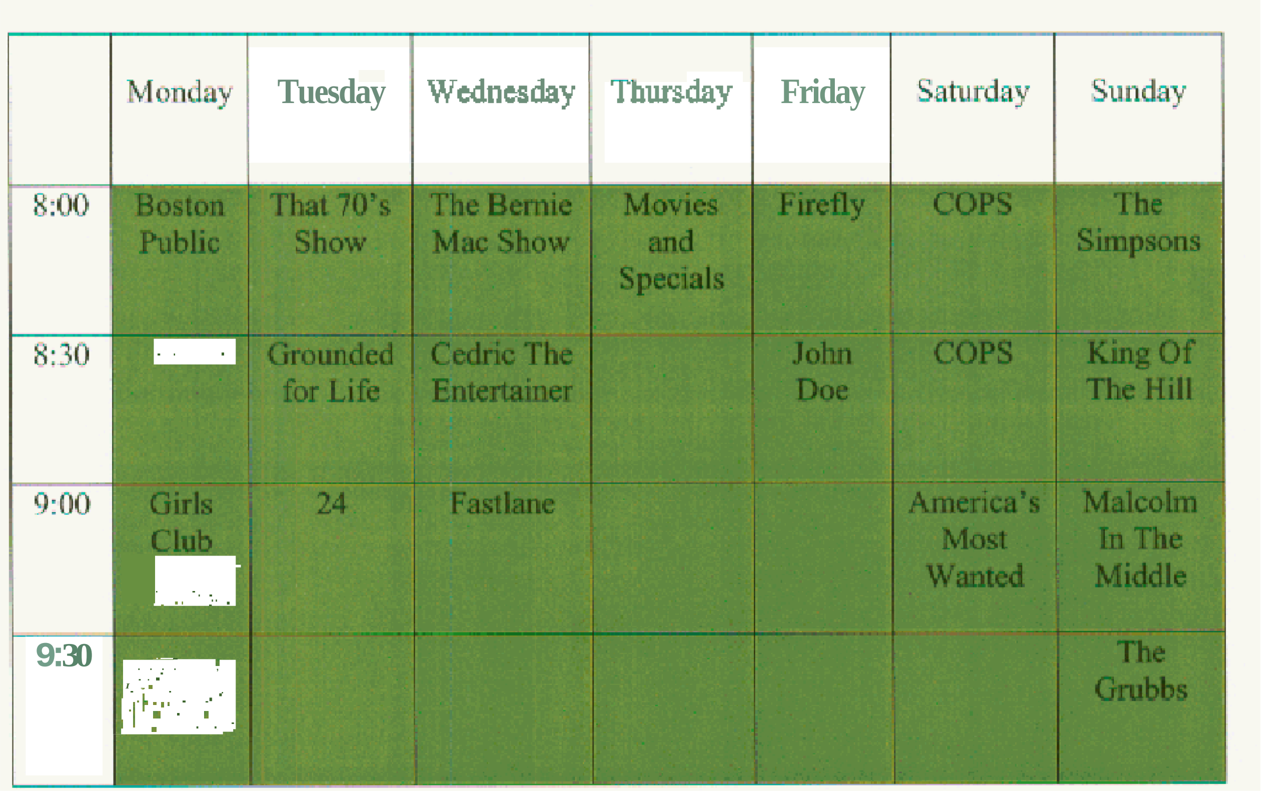
	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
8:00	Fear Factor	🟩 In-Laws	🟩 Ed	Friends	Providence	NBC Saturday Movie	🟩 American Dreams
8:30		Just Shoot Me	🟩	Scrubs			🟩
9:00	Third Watch	🟩 Frasier	The West Wing	Will And Grace	🟨 Dateline NBC		🟩 Law and Order: Criminal Intent
9:30		🟩 Hidden Hills		Good Morning Miami	🟨		🟩
10:00	🟩 Crossing Jordan	🟨 Dateline NBC	🟩 Law and Order	🟩 ER	🟩 Law And Order: SVU		🟩 Boomtown
10:30	🟩	🟨	🟩	🟩	🟩		🟩

NETWORK PRODUCED SHOW NOT IN HDTV

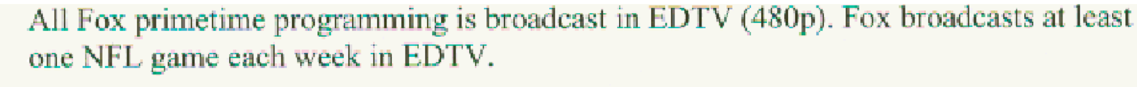
NBC broadcasts at least 11.5 hours per week in HDTV, 9.5 hours of which are in primetime. The Tonight Show with Jay Leno and The Conin O'Brian Show are also broadcast in HDTV.

Some movies such as Men in Black and Jurassic Park are also broadcast in HDTV. Previous HDTV broadcasts include the Triple Crown, selected portions of the 2002 Olympics, and selected NBA games.

Fox 2002-2003 Primetime Season (EDTV in green)



	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
8:00	Boston Public	That 70's Show	The Bernie Mac Show	Movies and Specials	Firefly	COPS	The Simpsons
8:30		Grounded for Life	Cedric The Entertainer		John Doe	COPS	King Of The Hill
9:00	Girls Club	24	Fastlane			America's Most Wanted	Malcolm In The Middle
9:30							The Grubbs



All Fox primetime programming is broadcast in EDTV (480p). Fox broadcasts at least one NFL game each week in EDTV.

Network listings updated December 2, 2002
Sources: Network Press Releases, HDTV Magazine, and TitmTV.com.

APPENDIX B

1. **DTV** Broadcast **Flag** Encryption Based Content Protection System Requirements

1.1. A system used for the purpose of protecting digital terrestrial broadcast television comprised of the following:

- Rights Expression
- Data encryption
- Authentication

1.2. The encryption-based system should protect flagged, copyright-protected information consistent with preventing unauthorized access to market digital terrestrial broadcast television by the public. The system may permit such flagged, copyright-protected information to be transmitted among a variety of consumer devices, including but not limited to single and multi-function devices as well as general-purpose devices such as personal computers, so long as such transmission and down-stream consumption is consistent with the policy. These devices may be interconnected using any one of a variety of protocols including but not limited to Internet Protocol, 1394, UPnP, and 802.11x, etc. The encryption-based system is responsible for enforcing the policy expressed as rights using cryptographic and authentication techniques. The copy protection policy information can either be independent of the technology, thus making policy and technology mutually independent, or implemented within the technology itself.

- Rights Expression: The policy may be expressible in a manner that can interoperate with an industry standard rights expression language (REL), but the only requirement is that a system adhere to the limitations of the policy such as XrML, if not transmitted directly in the XrML-like format.

- Encryption/Decryption: To protect content and insure it can only be accessed in usable form by authorized devices that adhere to the policy, appropriate cryptographic techniques based on a publicly described cryptographic algorithm should be used. It must be possible *to* implement the encryption/decryption algorithm in hardware and/or software. Furthermore, it should be reasonable to implement the encryption/decryption algorithm in small, low cost consumer electronics devices and for personal computers. Management of decryption keys must be controlled so that only specified persons may obtain access to the content consistent with the policy.

- Authentication: The authentication method must operate such that any source device participating in the exchange of protected media can determine the authenticity of a targeted device and such device’s ability to evaluate and enforce media rights described in the policy. It must be possible to implement the authentication method in hardware, software, or some combination.

1.3 Interoperability

The components of the system should be interoperable and consistent with appropriate related industry standards, enabling policy to be honored and content to be protected if it should move from one encryption-based copy protection system to another.

1.4. Strength

a) The encryption algorithm should be robust in that circumvention of the encryption algorithm should be difficult and serve to keep honest people honest.
b) If possible, the encryption algorithm should be such that detailed knowledge of a given implementation of this algorithm should not, in and of itself, be sufficient information to allow the production of circumvention devices.
c) In the case of circumvention, it should be possible to renew methods of protection, thus preventing future abuses of copy protected materials.
d) Should a particular device in a system be compromised, its future participation in receiving protected content should be revocable or replaceable.

1.5. Resistance to Product Obsolescence

- Products implementing the encryption algorithm should not become obsolete between the time that they are introduced in the market and the time that they may otherwise become obsolete due to market influences not related to copy protection.

    - For example, if a product provides a means to change the encryption algorithm, and if, in fact, the algorithm is changed in the future, then existing devices should be able to transmit to, and receive and play digital content from, devices complying with the requirements of the changed encryption algorithm, and future devices, complying with the requirements of the changed encryption algorithm, must be able to transmit to, and receive and play digital content from, older devices.